مجلة الجامعة الإسلامية (سلسلة الدراسات الإنسانية) المجلد السادس عشر، العدد الثاني، ص895 - ص923 يونيه 2008
ISSN 1726-6807, http://www.iugaza.edu.ps/ara/research/

مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة

د. عصام محمد البحيصي و **أ. حرية شعبان الشريف**
كلية التجارة – قسم المحاسبة ماجستير محاسبة
الجامعة الاسلامية – غزة - فلسطين

تاريخ استلام البحث: 2007/5/26م ، **تاريخ قبول البحث**: 2007/12/1م

ملخص: يهدف هذا البحث للتعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، والتعرف على أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر. و قد قام الباحثان بالاطلاع على الدراسات السابقة والأبحاث التي اهتمت في هذا المجال، ثم إعداد استبيان خاص تم توزيعه على البنوك العاملة في محافظات قطاع غزة، و من ثم تم تحليل البيانات التي تم جمعها؛ وبناء على ذلك تم استخلاص بعض النتائج التي أسهمت في التعرف على أهم المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، و التي من أهمها:(1) مخاطر نظم المعلومات المحاسبية المحوسبة، و ان كانت تحدث لدى البنوك العاملة في قطاع غزة، الا أنها تكرر بشكل غير كبير؛(2)عدد موظفي تكنولوجيا المعلومات في المصارف العاملة في قطاع غزة ؛ (3) حدوث مخاطر نظم المعلومات المحاسبية الالكترونية ترجع إلى أسباب تتعلق بموظفي البنك، نتيجة قلة الخبرة، الوعي والتدريب، اضافة إلى أسباب تتعلق بإدارة المصرف؛ نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الاجراءات والأدوات الرقابية المطبقة لدى المصرف؛ (4) المصارف العاملة في قطاع غزة تتبع اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية. و علىضوء نتائج الدراسة تم التوصل إلى مجموعة من التوصيات من أهمها : (1) من الضروري أن تدعم الادارة العليا للمصارف أمن المعلومات لديها و أن تعمل على إنشاء قسم خاص بتكنولوجيا المعلومات في كافة المصارف وتوفير كادر متخصص في تكنولوجيا المعلومات بحيث يكون له مندوبون في الفروع ذوي خبرة وكفاءة عالية لأجل العمل على حماية أمن نظم المعلومات المحاسبية لدى المصارف. و كذلك تطوير قدرات العاملين لديها في مجال امن المعلومات و حمايتها.(2) ضرورة وضع اجراءات تضمن استمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الأزمات، و ذلك من خلال استخدام تجهيزات منيعة أو مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها والحد من وقوعها. وكذلك العمل على تعمية أو تشفير المعلومات عند الحفظ والنقل والتخزين على مختلف الوسائط كي لا يتمكن أحد من اختراقها. (3) وضع ضوابط أمن ورقابة للمعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أم اتصالات سلكية ولاسلكية والإنترنت، والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية. و وجود خطة حماية أمنية شاملة والتي تنعكس في انخفاض النفقات الناتجة عن توظيف الحلول الجزئية للأمن.

Threats that affect computrised accounting information systems: Case study of the banks in Gaza Strip - Palestine

Abstract: The objective of this research is to investigate the threats that effect electronic accounting information systems in the working banks in the Gaza strip, to investigate the most important reasons that lead to the occurring of these threats, and to investigate the procedures that prevent the occurring of these threats. The researcheres use a special questionare that was disgined and distributed to serve the research objectives. The collected data was analysed using SpSS programme.T he following findings were reached: (1) the threats that affect the accounting information system: do exist , though it happened at low frequency at the the working banks in the Gaza strip; (2) the main reason for these threats is the lack of technological abitilty and qualifications of the banks empolyees (3) there is a low number of information technology employees in the banks in the Gaza strip, and the branches depend only on one employee whose job is to keep the operation of information systems, while specialized employees work in the main branch, an these branches are usually found in the West bank. Dependig on these findings, the following recommendations are presented (1) secure procedures that assure the work continuity and availability of information systems in crisis cases through using immune equipments that can be able to find present the threats before their occurrence. (2) perfect controlling security tools for information using all types including paper form, wire or wireless communications and Internet, and working on required laws for information systems security and information networks security. (3) increase the banks employees ability in IT and information security field .

1- مقدمة:

يعتبر العصر الحالي عصر ثورة المعلومات والاتصالات، حيث أدى تطور تكنولوجيا المعلومات إلى ازدياد حجم المعلومات التي يجب أن تعالج وتخزن وتقدم للنظام بشكل كبير، مما عقد عملية التحكم بها والسيطرة عليها، وقد انتشرت تطبيقات تكنولوجيا المعلومات في شتى المجالات وعلى جميع المستويات، ويعد التطور السريع في تكنولوجيا المعلومات والإنتشار الواسع للنظم والبرامج الصديقة للمستخدم، بالاضافة إلى رغبة المنشآت في إقتناء وتطبيق أحدث النظم والبرامج الإلكترونية دافعا أساسيا لإستخدام الحاسب الآلي وأداء العديد من المهام والوظائف المحاسبية بصورة أسرع وأدق، ولكن على الجانب الأخر فإن هذا التقدم التكنولوجي الهائل قد يحمل بين طياته العديد من المخاطر الهامة المتعلقة بأمن وتكامل النظم المحاسبية الإلكترونية؛ نظراً لأن التطور في الحاسبات وتكنولوجيا المعلومات لم يصاحبه تطوراً مماثلاً في الممارسات والضوابط الرقابية، كما لم يواكب ذلك تطوراً مماثلاً في معرفة وخبرات ووعي العاملين بتلك المنشآت؛ ولذلك فإن نظام المعلومات المحاسبي في أي منشأة يجب أن يتضمن وسائل وضوابط رقابية على البيانات كي يتم تقديم تقارير تحتوي على معلومات موثوق بها من

قبل مستخدمي نظام المعلومات. وللمحاسبين دور مهم في تطوير وتقييم مقاييس الرقابة والأمان في نظام المعلومات المحاسبي، فهم يعملون عن قرب مع مصممي النظم أثناء تطوير نظام المعلومات المحاسبي حتى يتم التأكد من أن مقاييس الرقابة والأمان مناسبة وكافية، وإدخال الحاسب الآلـي في نظام المعلومـات يؤثر على وسائـل الرقابة والأمـان للبيانـات.(الدهـراوي ،2003،ص159). ومن هنا تظهرمسئولية جديدة و كبيرة أمام إدارة نظم المعلومات في المنشأة وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل تلك النظم بشكل صحيح، مع التخطيط الدقيق لمواجهة جميع الأخطار التي يمكن أن تؤدي إلى تعطلها أوتوقفها عن العمل، وفي حال حدوث ذلك، التمكن من إعادة تشغيلها بأسرع وقت ممكن. وبالنظر إلى البيئة الفلسطينية نلاحظ انتقال العمل في المصارف العاملة في قطاع غزة من النظام اليدوي إلى النظام الإلكتروني؛ مما يتطلب من إدارة المصارف العمل على احكام الرقابة على العمل المصرفي لأجل الحفاظ على أمن نظم المعلومات المصرفية .

وعليه أتت هذه الدراسة للتعرف على المخاطر المختلفة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية والتعرف على أسباب حدوثها وإجراءات الحماية المتبعة لمواجهة تلك المخاطر.

2- مشكلة الدراسة

تعتبر البيئة التجارية الفلسطينية بيئة سريعة التطور من حيث اعتمادها على النواحي التكنولوجية، و خاصة قطاع المصارف الذي يعتمد يوما بعد يوم بشكل متزايد على نظم المعلومات المحوسبة؛ لتغطية جميع جوانب النشاط، خاصة المحاسبي منها الامر الذي يجعلها عرضة للاخطار التي تتعلق بهذا المجال. و حيث إن النظم المحاسبية الالكترونية تواجه العديد من المخاطر المتعلقة بالمدخلات والمخرجات والتشغيل، فقد جاءت هذه الدراسة كمحاولة للتعرف على أهم المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة، ودرجة تكرارها. و أسباب حدوثها، و معدلات حدوثها. و كذلك إجراءات الحماية التي تتبعها المصارف للحد من المخاطر التي تهدد نظم المعلومات المحاسبية.

3- أهداف الدراسة

تهدف هذه الدراسة إلى:

1- التعرف على طبيعة المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى بيئة المصارف العاملة في قطاع غزة ومعدلات تكرارها، و أسباب حدوثها.

2- التعرف على اجراءات الحماية التي تتبعها المصارف العاملة في قطاع غزة للحد من المخاطر التي تهدد نظم معلومات المحاسبية الإلكترونية.

3- التمييز بين مخاطر أمن نظم المعلومات وعدم كفاية الضوابط الرقابية لأمن تلك النظم.
4- التركيز على مخاطر مخرجات الحاسب الآلي وعدم إهمالها.

4- أهمية الدراسة

تنبع أهمية هذه الدراسة من أهمية الموضوع ذاته وتتلخص في النقاط التالية:

1- إن نظم المعلومات المحاسبة الإلكترونية قد أصبحت عرضة للعديد من المخاطر التى تهدد صحة وموثوقية ومصداقية وسرية وتكامل ومدى إتاحة و ملاءمة البيانات المالية والمحاسبية التى توفرها تلك النظم.
2- وجود خلط واضح وعدم تمييز بين مخاطر أمن نظم المعلومات وعدم كفاية الضوابط الرقابية لأمن تلك النظم لدى العديد من الباحثين.
3- حداثة هذه الدراسة حيث تعتبر (في حدود علم الباحثين) الدراسة الأولى من نوعها التي تطبق بشكل كامل على المصارف العاملة في قطاع غزة؛ وبالتالي تمكن المصارف من الإستفادة من نتائجها في تطوير أداء المصارف فيما يتعلق بالسيطرة على المخاطر؛ مما يعزز دورها في المجتمع وزيادة الثقة في الجهاز المصرفي بشكل عام.

5- فرضيات الدراسة

1- لا تحدث المخاطر المتعارف عليها في بيئة نظم المعلومات المحاسبية الالكترونية (مخاطر تتعلق بادخال البيانات، مخاطر تتعلق بالتشغيل، مخاطر تتعلق بالمخرجات و مخاطر تتعلق بالبيئة) بشكل متكرر في المصارف العاملة في قطاع غزة:
2- ترجع اسباب حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة إلى:

أ- أسباب تتعلق بموظفي البنك نتيجة لقلة الخبرة و الوعي والتدريب.
ب- اسباب تتعلق بادارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الاجراءات والادوات الرقابية المطبقة .

3- لا توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة

6- منهجية الدراسة

من أجل تحقيق أهداف الدراسة قام الباحثان بتصميم وتوزيع أستبانة، أعدت خصيصا لهذا الغرض. وتشتمل الاستبانة على قائمة تضم مجموعة المخاطر التي تهدد نظم المعلومات

المحاسبية المحوسبة كما استخلصها الباحثان من الدراسات السابقة الخاصة بالموضوع. و قبل توزيع الاستبانة على عينة الدراسة تم اختبار مدى صلاحيتها عبر تنفيذ الاجراءات التالية:-

1- **التحكيم**: فقد تم عرض الاستبانة في صورتها الأولية على بعض الأساتذة الأكاديميين و خبراء في اللغة العربية و من لهم خبرة وإطلاع في مجال نظم المعلومات المحاسبية لأجل الاسترشاد بآرائهم حول الفقرات التي تضمنتها الاستبانة. وقد اخذ الباحثان بآراء ونصائح المحكمين؛ حيث تم حذف بعض الفقرات، كما تم تعديل فقرات أخرى، حتى تم التوصل للصورة النهائية للاستبانة.

2 – **الصدق و الثبات**: فقد تم اجراء بعض التحليلات الاحصائية للاستبانة (تحليلات الصدق و الثبات). أما بالنسبة لتحليل الصدق، أي مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي إليه تلك الفقرة، فقد تم التحقق من صدق الاتساق الداخلي من خلال إيجاد معامل الارتباط الخطي لبيرسون بين كل فقرة من فقرات الاستبانة والدرجة الكلية للمجال الذي تنتمي إليه تلك الفقرة، وقد كانت النتائج ايجابية بشكل كبير، حيث دلت معاملات الارتباط المختلفة على أن هناك اتساق داخلياً للفقرات مع المجالات التي تنتمي إليها. أما فيما يتعلق بتحليل الثبات، فقد تحقق الباحثان من ثبات استبانة البحث من خلال طريقتي التجزئة النصفية ومعامل ألفاكرونباخ. و قد تبين لنا من نتائج التحليل التجزئة النصفية ان معامل ثبات الاستبانة بلغ 0.975 ، وأن معامل ألفاكرونباخ للاستبانة ككل بلغ 0.956 وهي قيم جيدة ودالة إحصائيا عند مستوى دلالة $\alpha = 0.01$، كما أن معاملات الارتباط والثبات ومعاملات ألفاكرونباخ لمجالات الاستبانة الخمس أيضاً مرتفعة ومعنوية إحصائيا؛ مما يؤكد ثبات الاستبانة وصلاحيتها للاستخدام.

أما من حيث عينة الدراسة فانها تتكون من مدراء المصارف والمحاسبين ورؤساء الأقسام ومراجعي نظم المعلومات الإلكترونية والمراجعين الداخليين والمراقبين في تلك المصارف ومهندسي وموظفي دوائر تكنولوجيا المعلومات. و قد تم توزيع عينة شاملة تشمل جميع اعضاء مجتمع العينة في جميع المصارف العاملة في قطاع غزة وفروعها باستثناء المؤسسة المصرفية والبنك العربي وذلك لاسباب خاصة بالمؤسستين. و قد تم توزيع 159 استبانة وقد تم استعادة 129 منها ليصل معدل الردود إلى 81% من إجمالي العينة. وقد تم استخدام اسلوب التحليل الوصفي(Descriptive Analysis) للبيانات التي تم تجميعها؛ للتعرف على الخصائص الأساسية لعينة ومتغيرات الدراسة، حيث اعتمدت الباحثة على المنهج الوصفي التحليلي، لأنه يعتبر من أنسب المناهج لمثل هذه الدراسة، كما تم إجراء بعض الاختبارات اللامعلمية Non-Parametric

Tests (مثل إختبار Sign Test) لإختبار فرضيات البحث وذلك من خلال استخدام برنامج (SPSS) الاحصائي.

7- الاطار النظري و الدراسات السابقة

تعتبر نظم المعلومات المحاسبية الإلكترونية من النظم التي تواجه العديد من المخاطر التي قد تؤثر على تحقيق أهداف تلك النظم؛ وذلك نظرا لاعتمادها على الحاسوب، حيث تزامن التطور الكبير للحاسبات وأنظمة المعلومات مع التطور في تكنولوجيا المعلومات وسرعة انتشار هذه المعلومات واستخدامها إلكترونيا، ولقد صاحب هذا التطور في استخدام المعلومات الإلكترونية العديد من المخاطر والمشاكل التي تؤثر على أمن المعلومات سواء كانت تلك المخاطر مقصودة أم غير مقصودة . وتعتبر المخاطر المقصودة أشد خطرا على أداء فعالية النظم. وتكمن خطورة مشاكل أمن المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية، أو تخريبها بالكامل؛ مما يؤدي إلى تعطيل الخدمات الحيوية للمنشأة، أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الاطلاع والتصنت على المعلومات السرية أو تغييرها الى خسائر مادية أو معنوية كبيرة.

هذا ويعتبر موضوع أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية من المواضيع الهامة والحديثة نسبيا، حيث إنه من خلال مراجعة الدراسات والأبحاث السابقة والمتعلقة بهذا الموضوع نجد أن هناك ندرة في العالم العربي حول هذا الموضوع مع توفر دراسات قليلة في العالم الغربي وهذا إن دل على شيء فإنما يدل على الحداثة النسبية لهذا الموضوع رغم أهميته الحيوية لكثير من المنشآت والمصارف. وتجدر الإشارة إلى أن الأبحاث القليلة التى تمت فى هذا الموضوع قد إستهدفت التعرف على المخاطر المحتملة التى قد تواجه أو تهدد أمن تلك النظم والتعرف على أسبابها ومحاولة تطوير قائمة تتضمن أهم المخاطر التى قد تواجه أمن النظم المحاسبية الإلكترونية، ومن ثم محاولة إختبار مدى جوهرية وأهمية تلك المخاطر فى الواقع العملى من خلال مجموعة من الدراسات الميدانية التى تمت فى هذا الشأن، وذلك من خلال التعرف على معدل تكرار حدوثها وحجم الخسائر المالية الناجمة عنها. و من اهم الدراسات في هذا المجال:

دراسة Loch et al. (1992) و هي بعنوان " Threats to Information Systems: Today'sReality and Yesterday's Understanding" . وتعد الدراسة من أوئل الدراسات فى هذا المجال، حيث قام Loch ورفاقه بعمل دراسة مسحية شملت 657 من مديرى نظم

مخاطر نظم المعلومات المحاسبية الإلكترونية

المعلومات الإدارية فى الولايات المتحدة، إستهدفت إستكشاف مدى إدراك مديرى نظم المعلومات الإدارية فيما يتعلق بالمخاطر الأمنية التى تواجه أمن النظم المحاسبية الإلكترونية فى بيئة الحاسبات الشخصية والحاسبات الكبيرة وكذلك شبكة الحاسبات الإلكترونية. ولقد قام Loch ورفاقه بتطوير قائمة تضمنت إثنى عشر خطرا من المخاطر المحتملة التى قد تواجه أمن نظم المعلومات المحاسبية الإلكترونية. ولقد أوضحت نتائج تلك الدراسة أن الكوارث الطبيعية والأحداث غير المقصودة لموظفى المنشأة قد تم تصنيفها ضمن الثلاثة مخاطر الهامة فى جميع بيئات تكنولوجيا المعلومات، كما أعطى المشاركون فى الدراسة أهمية أكبر للمخاطر الداخلية مقارنة بالمخاطر الخارجية لأمن نظم المعلومات المحاسبية الإلكترونية، كما أظهرت الدراسة أن التدمير غير المتعمد للبيانات والإدخال غير المتعمد لبيانات غير سليمة بواسطة موظفى المنشأة وكذلك الرقابة غير الكافية على الوسائل مثل الأشرطة والأقراص الممغنطة تعد أهم ثلاثة مخاطر تواجه أمن نظم المعلومات فيما يتعلق بأجهزة الحاسب الشخصية, و أن أهم ثلاثة مخاطر تتعلق بأجهزة الحاسب الألى الكبيرة تتمثل فى: الإدخال غير المتعمد لبيانات غير سليمة من قبل موظفى المنشأة، الكوارث الطبيعية، والتدمير غير المتعمد للبيانات بواسطة موظفى المنشأة، بينما أظهرت الدراسة أن الكوارث الطبيعية والدخول غير المصرح به للبيانات/ النظام من قبل أطراف خارجية (قراصنة المعلومات) وضعف الأدوات الرقابية المادية تعد أهم ثلاثة مخاطر تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى بيئة شبكة الحاسب الآلى .

دراسة **Ryan and Bordoloi (1997)** و هي بعنوان "Evaluating Security Threats in Mainframe and Client / Server Environments". وهي دراسة تطبيقية لتقييم مخاطر أمن نظم المعلومات فى النظم المحاسبية الإلكترونية فى المنشأت التى تحولت من نظام أجهزة الحاسوب الكبيرة إلى نظام خدمة العملاء، ولقد قام الباحثان بتطوير قائمة شملت خمسة عشر من المخاطر المحتملة التى قد تهدد أمن نظم المعلومات الإلكترونية، و توزيعها على مائة وعشرين شركة من الشركات الكبيرة والمتوسطة الحجم فى الولايات المتحدة، . وأشارت نتائج تلك الدراسة إلى وجود فروق جوهرية (عند مستوى معنوية $P = 0.05$) بين المنشأت التى لديها نظام أجهزة الحاسوب الكبيرة وتلك التى تطبق نظام خدمة العملاء فيما يختص بمخاطر أمن نظم المعلومات المحاسبية الإلكترونية التالية: التدمير غير المتعمد للبيانات بواسطة موظفى المنشأة، الإدخال غير المتعمد لبيانات خاطئة بواسطة موظفى المنشأة، التدمير المتعمد للبيانات بواسطة موظفى المنشأة، الإدخال المتعمد لبيانات خاطئة بواسطة موظفى المنشأة، الخسائر الناجمة عن عدم إعداد نسخ إضافية (Backups) أو الرقابة على ملفات الدخول للنظام (Log Files)، أو فشل النظام وسقوط

الشبكات، وقد أعترف الباحثان أن قائمة المخاطر المقترحة من قبلهم قد تضمنت بعض العناصر التى لايمكن إعتبارها ضمن مخاطر أمن نظم المعلومات بالمعنى الدقيق .

دراسة Dhillon (1999) وهي بعنوان "Managing and controlling computer misuse",

تتعلق بطبيعة اختراقات أمن المعلومات التي حدثت في أماكن مختلفة من العالم، حيث ناقش فيها العديد من خسائر أمن المعلومات التي تنتج من الاحتيال على أنظمة الحاسوب، حيث إنه يمكن تفادي تلك الخسائر؛ إذا تبنت المنظمات نظرة أكثر واقعية في التعامل مع مثل هذه الحوادث بالإضافة إلى تبني نظرة تحكم أمنية تضع تأكيدا متساويا للتدخلات الشكلية والرسمية والتقنية لأنظمتها الإلكترونية، ومن خلال نتائج الدراسة اقترح بأن تطبيق السيطرة، كما هو معرف في سياسة أمن المعلومات، يردع حقيقية سوء استعمال الحاسوب، كما أن ارتكاب الاحتيال على أنظمة الحاسوب من قبل المستخدمين الداخليين، تعرف كمشاكل التخزين، واحتيال أنظمة الحاسوب عالية التقنية يصعب منعها خاصة إذا امتزجت بالمعاملات القانونية .

دراســـة Siponen (2000) و هـــي بعنـــوان " A conceptual Foundation for "Organizational Information Security Awareness". و التي قدمت تــصورا لبرنـــامج وعي أمن المعلومات في المؤسسات؛ وذلك لتقليل أخطاء المستخدمين؛ ولتحسين فعاليـــة ســيطرة الأمن المطبقة، وقد توصل الباحث إلى أن تقنيات أو إجراءات أمـــن المعلومـــات تفقـــد فائـــدتها الحقيقية؛ إذا تم إساءة استخدامها، أو تم تفسيرها بطريقة خاطئة أو تم تطبيقها بشكل غير صـــحيح من قبل المستخدمين.

دراسة Abu-Musa (2001) وهي بعنوان " A conceptual Foundation for Organizational "Information Security Awareness". حيث قام الباحث بعمل دراسة تطبيقية؛ لإستكشاف وإختبار المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى القطاع المصرفى بجمهوربة مصر العربية، حيث تم عمل دراسة مسحية شملت جميع البنوك الرئيسة العاملة بجمهورية مصر العربية للتعرف على أراء كل من رؤساء أقسام الحاسب الألى ورؤساء أقسام المراجعة الداخلية، فيما يختص بالمخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى البنوك التى يعملون بها. وتشير نتائج الدراسة إلى أن الإدخال غير المتعمد لبيانات غيرصحيحة من قبل موظفى البنوك، التدمير غير المتعمد للبيانات من قبل موظفى البنوك، إدخال فيروس الكمبيوتر إلى النظام، الكوارث الطبيعية والكوارث التى هى من صنع الإنسان، إشتراك بعض الموظفين فى إستخدام نفس كلمة السر، وكذلك توجية البيانات والمعلومات إلى أشخاص غير مخول لهم بإستلامها تعد من أهم المخاطرالتى تواجه أمن نظم

المعلومات المحاسبية الإلكترونية فى البنوك المصرية. وتجدر الإشارة إلى أنه فى جميع الحالات فإن رؤساء أقسام المراجعة الداخلية قد أعطوا تقديرات أعلى لمعدلات حدوث تلك المخاطر فى البنوك التى يعملون بها مقارنة بتقديرات رؤساء أقسام الحاسب الألى، وتشير نتائج الدراسة أنه لا توجد إختلافات جوهرية بين أنواع البنوك المختلفة إلا فيما يختص بالمرور غير المرخص به للبيانات/ النظام من قبل أطراف خارجية (قراصنة المعلومات) .

دراسة (Whitman (2003 و هي بعنوان " Enemy at the Gate: Threats to InformationSecurity و قد ركزت على الإجابة على ثلاثة فقرات، الأولى تتعلق بحصر التهديدات التي تواجه أمن المعلومات، و الثانية تتعلق بدرجة خطورة هذه التهديدات، و الثالثة تتعلق بعدد مرات حدوثها (شهريا)، حيث قام الباحث بعمل تقييم لعدد من الأبحاث والمقالات في مجال أمن المعلومات، وحصر التهديدات التي تواجه أمن المعلومات.حيث قام الباحث بعمل دراسة مسحية شملت ألف موظف أغلبهم من مدراء نظم المعلومات، والمدراء و المشرفين. وأوضحت الدراسة أن التهديد حقيقي، وخطورته عالية، وأن الأنظمة المعرضة للتهديد يصعب حمايتها، وركزت الدراسة على أن الإدارة يجب أن تكون مطلعة أكثر على تهديدات أمن المعلومات، ويجب أن يزداد وعيها في كل المجالات، وأن مستوى فهمهم العام لأمن المعلومات متأصل من خلال علاقتها مع البيئة التي تعمل بها .

دراسة (Abu-Musa (2004 و هي بعنوان " Important Threats to Computerized Accounting ."Information Systems: An empirical Study on Saudi Organizations و هي دراسة تطبيقية للتعرف على المخاطر الهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى المنشأت السعودية، ولقد أظهرت نتائج الدراسة أن نسبة عالية من المنشأت التى شاركت فى الإستقصاء قد عانت من وجود خسائر مالية كبيرة؛ نتيجة بعض التعديات على أمن نظم المعلومات المحاسبية بها سواءً من قبل أطراف داخلية أم أطراف خارجية، كما أوضحت الدراسة أن كثيراً من تلك التلاعبات والإختلاسات والتعديات على أمن نظم المعلومات المحاسبية قد تم إكتشافها عن طريق الصدفة؛ نتيجة لعدم كفاية وفعالية الأدوات والضوابط الرقابية المطبقة، وأن معظم الإختلاسات والتلاعبات التى تم إكتشافها قد تمت تسويتها داخلياً ولم يتم الإفصاح أو التقرير عنها للجمهور حفاظاً على سمعة الشركة وتحسين صورتها فى السوق . أما فيما يختص بمدى إدراك المنشأت السعودية للمخاطر الهامة التى تهدد نظم المعلومات المحاسبية ومعدلات تكرار حدوث تلك المخاطر بها، أشارت نتائج الدراسة إلى أن أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشآت السعودية هي: الإدخال

المتعمد وغير المتعمد لبيانات غير صحيحة بواسطة موظفي المنشآت، إدخال فيروسات الكمبيوتر إلى النظام المحاسبي، مشاركة الموظفين في استخدام نفس كلمات السر، طمس أو تدمير مخرجات الحاسب الآلي، الكشف غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الأوراق، وكذلك توجيه المطبوعات والمعلومات إلى أشخاص غير مخول لهم الإطلاع علي تلك المعلومات.

ومن خلال الاطلاع على الدراسات السابقة قام الباحثان بتصنيف المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية بشكل عام إلى أربعة أصناف رئيسة:

أولاً: مخاطر المدخلات

وهي المخاطر التي تتعلق بأول مرحلة من مراحل النظام وهي مرحلة ادخال البيانات إلى النظام الآلي وتتمثل تلك المخاطر في البنود التالية:-

1- الادخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.
2- الادخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.
3- التدمير غير المتعمد للبيانات بواسطة الموظفين.
4- التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.

ثانياً: مخاطر تشغيل البيانات

وهي المخاطر التي تتعلق بالمرحلة الثانية من مراحل النظام وهي مرحلة تشغيل ومعالجة البيانات المخزنة في ذاكرة الحاسب وتتمثل تلك المخاطر في البنود التالية:-

1- الوصول غير الشرعي (غير المرخص به) للبيانات والنظام بواسطة الموظفين.
2- الوصول غير الشرعي للبيانات والنظام بواسطة أشخاص من خارج المنشأة.
3- اشتراك العديد من الموظفين في نفس كلمة السر.
4- إدخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام.
5- اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.

ثالثاً: مخاطر مخرجات الحاسب.

تتعلق تلك المخاطر بمرحلة مخرجات عمليات معالجة البيانات وما يصدر عن هذه المرحلة من قوائم للحسابات أو تقارير وأشرطة ملفات ممغنطة وكيفية استلام تلك المخرجات وتتمثل تلك المخاطر في البنود التالية:-

1- طمس أو تدمير بنود معينة من المخرجات.
2- خلق مخرجات زائفة/ غير صحيحة.

3- سرقة البيانات/ المعلومات.
4- عمل نسخ غير مصرح (مرخص) بها من المخرجات.
5- الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.
6- طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.
7- المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخولين باستلام نسخة منها.
8- تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.

رابعاً: مخاطر بيئية

وهي المخاطر التي تحدث بسبب عوامل بيئية، مثل: الزلازل والعواصف والفيضانات والأعاصير، و المتعلقة بأعطال التيار الكهربائي والحرائق؛ وسواء كانت تلك الكوارث طبيعية أم غير طبيعية فإنها قد تؤثر على عمل النظام المحاسبي وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة مما يؤثر على أمن وسلامة نظم المعلومات المحاسبية الالكترونية .

8- الدراسة الميدانية ونتائج التحليل الاحصائي

في هذا المبحث نستعرض خصائص عينة البحث و اهم نتائج التحليل الاحصائي التي تم الحصول عليها عبر تحليل البيانات التي شملتها الاستبانة.

خصائص العينة.

وتشمل خصائص العينة، خصائص الاشخاص الذين قاموا بتعبئة لاستبيان و كذلك خصائص المؤسسات التي يعملون بها، و هذه الخصائص موضحة في الجداول (2-1).

جدول رقم (1)

خصائص معبئي الاستبيان (المؤهل العلمي و المسمى الوظيفي و الخبرة)

المؤهل العلمي	%	المسمى الوظيفي	%	الخبرة	
ثانوية عامة	2.3%	محاسب	11.6%	اقل من 3 سنوات	27.1%
دبلوم	8.5%	مراجع نظم معلومات الكترونية	7.0%	6 - 3 سنوات	13.2%
بكالوريوس	84.5%	مراجع داخلي	10.9%	10- 7سنوات	25.6%
ماجستير	4.7%	رئيس قسم	27.1%	من 15 - 11 سنة	20.9%
		مدير	6.2%	أكثر من 15 سنة	13.2%
		مراقب عام	8.5%		

		غير ذلك	28.7%		
الإجمالي	100%	**الإجمالي**	100%	**الإجمالي**	100%

يتضح من خلال الجدول رقم (1) أن أغلبية المشاركين في الاستقصاء كانوا من حملة شهادة البكالوريوس وأن عددا قليلا منهم كانوا من حملة شهادة الماجستير وهذا يعكس واقع الهيكل الوظيفي لموظفي البنوك الذين هم في اغلبهم من حملة درجة البكالوريوس مما يعني أن عينة الدراسة تعد عينة ممثلة للهيكل الوظيفي في المصارف العاملة في قطاع غزة . كما ان هؤلاء الموظفين هم من مختلف التخصصات ذات العلاقة موضوع البحث. من ناحية أخرى فإننا نلاحظ أن حوالي 60% من المشاركين في الإستقصاء كانت خبرتهم تزيد عن سبع سنوات، مما يعطي دعما وثقة أكبر لنتائج الاستبانة نتيجة الخبرة الجيدة التي يتمتع بها هؤلاء الموظفين في العمل المصرفي.

جدول رقم (2)

خصائص البنوك (النظام المحاسبي و عدد المحاسبين و المتخصصين في نظم المعلومات)

نوع البنك	نسبة %	النظام المحاسبي بالبنك	نسبة %	عدد المتخصصين في نظم المعلومات	نسبة %
تجاري	58%	يدوي	0%	1-5	77.5%
متخصص	25%	آلي كامل	79%	6-10	16.3%
اسلامي	17%	خليط	21%	11-15	4.7%
				أكثر من20	1.6%
الإجمالي	100%	**الإجمالي**	100%	**الإجمالي**	100%

من خلال الجدول رقم (2) يتضح أن العينة تمثل جميع انواع البنوك العاملة في قطاع غزة، وبنسبة تكاد تكون هي نفس نسبة توزيعها على ارض الواقع. من ناحية أخرى فان الأغلبية العظمى من المصارف (79%) لديها نظام محاسبي آلي في حين أن البقية لديها نظام نصف آلي. أما من ناحية عدد موظفي نظم المعلومات فإننا نلاحظ أنه في عدد كبير من المصارف يتراوح هذا العدد من 1-5، و في اغلبها كان عددالموظفين هو موظف واحد فقط مختص بتكنولوجيا المعلومات ومهمته تشغيل النظام فقط. وهذا مؤشر واضح على نقص عدد العاملين في مجال تكنولوجيا المعلومات في المصارف الفلسطينية. كما ان الاختلاف الواضح في أعداد المحاسبين العاملين في تلك المصارف قد يكون مؤشرا على اختلاف أحجام المصارف و حجم العمل فيها.

اختبار الفرضيات

لاختبار فرضيات الدراسة فقد تم استخدام اختبـار الإشـارة اللامعلمـي (Sign Test) والذي يعتبر أحد بدائل اختبار(t) لعينة واحدة المعلمي، إذ انه يستخدم للتحقق من مطابقة وسـيط عينة مختارة من مجتمع إحصائي مع وسيط ذلك المجتمع، كما أن اختبار الإشارة لا يعتمد علـى قيمة الفرق بين الدرجات والوسيط العام وإنما يتعامل فقط مع الإشارات من حيث كونها موجبة أو سالبة أو تأخذ صفراً والذي لا يدخل في المعالجة الإحصائية لأنه يعد محايداً، ولذلك فإن اختبـار الإشارة يستخدم لتحديد اتجاه الفروق بين آراء أفراد العينة. (عفانة، 1998، ص62-63).وقد تم إستخدام اختبار الإشارة لاختبار فرضيات الدراسة من خلال اختبار ما إذا كان وسيط آراء أفـراد العينة على كل عبارة من عبارات الاستبانة، وكذلك على المجالات ككل يختلف إحـصائياً عـن وسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (3) والتي تمثل الرأي (متـردد) فـي المجالين الثاني و الثالث، و الصفة (أكثر من مرة شهريا إلى مرة اسبوعيا) فـي المجـال الأول، لأجل معرفة ما إذا كانت هناك موافقة جوهرية ومعنوية احصائياً من أفراد العينة على عبـارات الاستبانة أم لا.

وقد تم استخدام اختبار الإشارة اللامعلمي؛ نظراً لأن متغيرات الاستبانة (العبارات) هي متغيرات رتبية وبالتالي لا تناسبها الاختبارات المعلمية كاختبار (t) وإنمـا تـم الاستعاضـة عـن ذلـك بالاختبارات اللامعلمية لعينة واحدة وأفضلها وأكثرها مناسبة لبيانات الدراسة هو اختبار الإشارة. و قد تم استخدام مقياس ليكرت الخماسي وقد تم ترميز هذا المقياس كما يلي:

موافق بشدة	موافق	متردد	غير موافق	غير موافق بشدة
5	4	3	2	1

وبالتالي كلما اقتربنا من الدرجة (5)؛ ازدادت شدة الموافقة على العبارة في حين تـزداد شدة المعارضة كلما اقتربنا من الدرجة (1) أما إذا اقتربنا من الدرجة (3)؛ فإن ذلك يكـون فـي الاتجاه المتردد. و هذا المقياس استخدم في المجالين الثاني و الثالث، اما في المجـال الاول فقـد كان المقياس المستخدم حول عدد مرات وقوع مخاطر نظم المعلومات كما يلي:

أقل من مرة واحدة سنوياً	من مرة سنوياً إلى مرة شهرياً	اكثر من مرة شهرياً إلى مرة اسبوعيا	اكثر من مرة أسبوعيا إلى مرة يومياً	اكثر من مرة يومياً أو بصفة متكررة
5	4	3	2	1

وبالتالي كلما اقتربنا من الدرجة (5)؛ فان عدد مرات حدوث المخـاطر يـنخفض الـى درجة انعدام حدوث المخاطر عند الدرجة (5)، ويزداد عدد مرات حدوث تلك المخـاطر؛ كلمـا

اقتربنا من الدرجة (1) أما إذا اقتربنا من الدرجة (3)؛ فإن ذلك يعني ان عـــدد مـــرات حـــدوث مخاطر نظم المعلومات في البنك متوسطا نسبيا.

1. اختبار الفرضية الرئيسية الأولى والتي تنص على أنه:

لا تحدث المخاطر المتعلقة بإدخال البيانات، التشغيل، المخرجات و بالبيئة بشكل متكرر في المصارف العاملة في قطاع غزة.

وتشير الفرضية الإحصائية العدمية (H0) إلى انعدام حدوث مخاطر نظـــم المعلومـــات بشكل متكرر في المصارف العاملة في قطاع غزة فيما لو كانت آراء أفراد العينة أقل أو تـــساوي الدرجة (3) و التي تمثل الخيار (أكثر من مرة شهرياً إلى مرة أسبوعيا). أما الفرضـــية البديلـــة (H1) فتشير إلى انعدام أو عدم حدوث مخاطر نظم المعلومات بشكل متكـــرر فـــي المـــصارف العاملة في قطاع غزة فيما لو كانت آراء أفراد العينة اكبر من الدرجة (3) و التي تمثـــل الخيـــار (أكثر من مرة شهرياً إلى مرة أسبوعيا). وسيتم اجراء الاختبار الاحـــصائي و تحديـــد مـــستوى المعنوية على أساس ذيل واحد و هو الذيل الأعلى كما هو واضح من الفرضية البديلة الـــسابقة، كما سيتم اختبار الفرضية الإحصائية السابقة لكل نوع من أنواع المخاطر الأربعة التي وردت في الفرضية البحثية السابقة؛ لمعرفة مدى تكرار حدوث تلك المخاطر في المـــصارف العاملـــة فـــي قطاع غزة وذلك كما هو موضح في الجدول رقم (3).

جدول رقم (3)

نتيجة اختبار الإشارة للمجال الأول الخاص بمخاطر نظم المعلومات المحاسبية الإلكترونية

انواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	الوسيط العام
مخـــــاطر الإدخال	1	126	2	129	11.003-	0.000	5
مخـــــاطر التشغيل	0	126	3	129	11.136-	0.000	5
مخـــــاطر المخرجات	0	126	3	129	11.136-	0.000	5
مخـــــاطر البيئة	0	128	1	129	11.225-	0.000	5

مستوى المعنوية الإحصائية حسب عند a = **0.05**

مخاطر نظم المعلومات المحاسبية الإلكترونية

من خلال الجدول رقم (3) يلاحظ أن قيمة اختبار الإشارة (z) معنوية إحصائياً عند مستوى دلالة (0.05)؛ مما يعني أن هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على كل نوع من أنواع مخاطر نظم المعلومات المحاسبية في المصارف العاملة في قطاع غزة ، ووسيط المقياس المستخدم في استبانة الدراسة، وهو الدرجة (3) ويعزز هذه النتيجة أن الوسيط العام لآراء أفراد العينة على كل نوع من أنواع المخاطر الأربعة في الجدول بلغ (5) وهي تمثل انعدام أو ندرة تكرار تلك المخاطر في المصارف العاملة في قطاع غزة حسب المقياس المستخدم في استبانة الدراسة. وبالتالي نستنتج من ذلك أن مخاطر نظم المعلومات المحاسبية الإلكترونية الأربعة لا تحدث بشكل متكرر؛ وبناء على ذلك نقبل الفرضية البحثية الأولى و التي نصت على أن مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة لا تحدث بشكل متكرر، وبذلك فإن تلك المخاطر على الرغم من عدم حدوثها بشكل متكرر فإنها قائمة بحكم طبيعة العمل المصرفي الألي الذي يتطلب توفير اجراءات حماية كافية.

وللوقوف على اراء افراد العينة حول مدى حدوث المخاطر التي تتضمنها كل نوع من انواع المخاطر الاربعة؛ فقد تم إيجاد اختبار الإشارة لكل عبارة على حدة من العبارات التي تضمنها المجال الأول و المتعلق بالمخاطر التي تهدد نظم المعلومات المحاسبية وذلك كما هو موضح بالجدول رقم(4)

جدول رقم (4)

نتيجة اختبار الإشارة لعبارات المجال الأول الخاص بمخاطر نظم المعلومات المحاسبية

عبارات المجال الأول (مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.	15	93	21	129	7,409-	0.000	4
الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.	2	126	1	129	10.872-	0.000	5
التدمير غير المتعمد للبيانات بواسطة الموظفين.	0	126	3	129	11.136-	0.000	5

عبارات المجال الأول (مخـــاطر نظـــم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
التـــدمير المتعمـــد (المقصود) للبيانات بواسطة الموظفين.	0	126	3	129	11.136-	0.000	5
المرور (الوصـــول) غير الشرعي (غير المـــرخص بـــه) للبيانـــات / النظـــام بواسطة الموظفين.	1	125	3	129	10.958-	0.000	5
المرور غير الشرعي (غير المرخص به) للبيانـــات / النظـــام بواسطة أشخاص من خارج المنشأة.	1	127	1	129	11.049-	0.000	5
إشراك الموظفين في كلمة السر .	1	119	9	129	10.681-	0.000	5
إدخـــال فيـــروس الكمبيـــوتر للنظـــام المحاسبي.	0	127	2	129	11.181-	0.000	5
اعتـــراض وصـــول البيانات من اجهـــزة الخوادم إلى اجهـــزة المستخدمين.	1	121	7	129	10.744-	0.000	5
طمس أو تدمير بنود معينـــــة مـــــن المخرجات.	1	126	2	129	11.003-	0.000	5
خلـــق مخرجـــات زائفة/ غير صحيحة.	0	127	2	129	11.181-	0.000	5
ســـرقة البيانـــات /المعلومات.	1	125	3	129	10.958-	0.000	5

عبارات المجال الأول (مخـــــاطر نظـــم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
عمـــل نـــسخ غيـــر مصرح (مـــرخص) بها من المخرجات.	2	124	3	129	10.780-	0.000	5
الكـــــشف غيـــــر المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعهـــا علـــى الورق.	5	122	2	129	10.293-	0.000	5
طبـــع و توزيـــع المعلومات بواســطة أشـــخاص غيـــر مصرح لهم بذلك.	33	120	6	129	10.459-	0.000	5
المطبوعـــــــات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم (ليس لهم الحق) في اســتلام نـــسخة منها.	0	119	10	129	10.817-	0.000	5
تـــسليم المـــستندات الحـــساسة إلـــى أشخاص لا تتـــوافر فيهم الناحية الأمنيـــة بغرض تمزيقهـــا أو التخلص منها.	3	119	7	129	10.412-	0.000	5
الكوارث الطبيعيـــة مثـــل الحرائـــق، الفيضانات أو انقطاع مصدر الطاقة.	0	126	3	129	11.136-	0.000	5

عبارات المجال الأول (مخـــاطر نظـــم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
الكـــوارث غيـــر الطبيعية والتي هـــي من صنع الإنـــسان مثـــل الحرائـــق، أو الفيضانات.	0	126	3	129	-11.136	0.000	5

مستوى المعنوية الإحصائية حسب عند a = 0.05

يلاحظ من خلال الجدول رقم (4) أن قيمة اختبار الإشارة (z) معنوية إحصائياً في كافة العبارات؛ ما يعني أن هناك فرق معنوي احصائياً بين وسيط آراء أفراد العينة على كـــل عبـــارة ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (3) كما ان وسيط آراء أفراد العينـــة في جميع العبارات كان 5 باستثناء العبارة الاولى فقد كان (4)؛ مما هذا يعني نـــدرة او انعـــدام حدوث المخاطر.

2- اختبار الفرضية الرئيسة الثانية والتي تنص على أنه:

ترجع اسباب حدوث المخاطر التي تهدد نظم المعلومات المحاســبية الإلكترونيـــة فـــي المصارف العاملة في قطاع غزة إلى:

أ- اسباب تتعلق بموظفي البنك؛ نتيجة لقلة الخبرة و الوعي والتدريب.

ب- اسباب تتعلق بادارة المصرف؛ نتيجة لعدم وجود سياسات واضـــحة ومكتوبـــة، وضـــعف الاجراءات والادوات الرقابية المطبقة.

لاختبار الفرضية السابقة فقد تم استخدام اختبار الإشارة؛ لمعرفة ما إذا كانت هناك فروقا معنويـــة إحصائياً بين وسيط آراء أفراد العينة على المجال الثاني والمتعلق باسباب حدوث مخـــاطر نظـــم المعلومات المحاسبية ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (3) والتي تمثل صفة (متردد)؛ وذلك لتحديد ما إذا كانت هناك موافقة جوهرية من قبل أفراد العينة على اســـباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية و التي تضمنها المجال الثاني بشكل عام ام لا. وفيما يلي نتيجة اختبار الإشارة على المجال الثاني ككل مصنفا في فئتين هما اســـباب تتعلـــق بالموظفين و اسباب تتعلق بادارة المصرف. وتشير الفرضية الإحصائية العدمية (H0) إلى تردد أو اعتراض افراد العينة على اسباب حدوث مخاطر نظم المعلومات فيما لو كانـــت آراء أفـــراد

العينة اقل او تساوي الدرجة (3) حسب المقياس المستخدم في استبانة الدراسة، أما الفرضية البديلة (H1) فاشارت إلى موافقة افراد العينة على اسباب حدوث مخاطر نظم المعلومات المحاسبية فيما لو كانت آراء أفراد العينة اكبر من الدرجة (3)؛ وسيتم اجراء الاختبار الاحصائي و تحديد مستوى المعنوية على اساس ذيل واحد و هو الذيل الاعلى كما هو واضح من الفرضية البديلة السابقة، وفيما يلي نتيجة الاختبار.

جدول رقم (5)

نتيجة اختبار الإشارة للمجال الثاني الخاص بأسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية

انواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	الوسيط العام
اسباب تتعلق بالموظفين	42	66	21	129	2.213-	0.027	4
اسباب تتعلق بإدارة المصرف	46	70	13	129	2.135-	0.033	4

مستوى المعنوية الإحصائية حسب عند a = 0.05

من خلال الجدول رقم (5) يلاحظ أن قيمة اختبار الإشارة (z) معنوية إحصائياً عند مستوى دلالة (0.05)؛ هذا يعني أن هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على كلا النوعين من اسباب حدوث مخاطر نظم المعلومات المحاسبية ، ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (3) ويعزز هذه النتيجة أن الوسيط العام لآراء أفراد العينة على كلا النوعين من اسباب حدوث مخاطر نظم المعلومات المحاسبية بلغ (4) وهي تمثل درجة الموافقة حسب المقياس المستخدم في استبانة الدراسة. وبالتالي نستنتج من ذلك ان افراد العينة يرون ان اسباب حدوث مخاطر نظم المعلومات المحاسبية ترجع لاسباب تتعلق بموظفي المصرف، و اسباب أخرى تتعلق بادارة المصرف بشكل عام. وبناء على ذلك نقبل الفرضية البحثية الثانية و التي نصت على ان اسباب حدوث مخاطر نظم المعلومات المحاسبية ترجع إلى اسباب تتعلق بموظفي البنك؛ نتيجة لقلة الخبرة و الوعي والتدريب، و اسباب تتعلق بادارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الاجراءات والادوات الرقابية المطبقة.

وللوقوف على اراء افراد العينة حول اسباب حدوث المخاطر الواردة في المجال الثـاني بـشكل مفصل فقد تم إيجاد اختبار الإشارة لكل سبب من الاسباب التي تضمنها المجال الثاني و المتعلقـة بحدوث المخاطر التي تهدد نظم المعلومات المحاسبية وذلك كما يظهر في الجدول رقم (6).

جدول رقم (6)

نتيجة اختبار الإشارة لكل عبارة من عبارات المجال الثاني الخاص بأسباب حدوث مخاطر نظم المعلومات المحاسبية

عبارات المجال الثاني (أسباب حدوث مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
عدم كفاية وفعالية الأدوات والضوابط الرقابية المطبقة في البنك.	40	74	15	129	3.091-	0.001	4
ضعف نظم الرقابة الداخلية في البنك وعدم فعاليتها.	46	65	18	129	1.708-	0.044	4
اشتراك بعض الموظفين في استخدام نفس كلمات السر.	62	55	12	129	0.555-	0.2895	3
عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات.	44	70	15	129	2.341-	0.0095	4
عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم	43	74	12	129	2.774-	0.003	4

مخاطر نظم المعلومات المحاسبية الإلكترونية

عبارات المجال الثاني (أسباب حدوث مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
المعلومات المحاسبية بالبنك.							
عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في البنك.	47	69	13	129	1.950-	0.0255	4
ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب الآلي.	53	65	11	129	11013-	0.1555	3
عدم وجود سياسات واضحة ومكتوبة فيما يختص بأمن نظم المعلومات المحاسبية في البنك.	45	68	16	129	2.070-	0.019	4
عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسئوليات والصلاحيات لكل	50	71	8	129	1.818-	0.0345	4

عبارات المجال الثاني (أسباب حدوث مخاطر نظم المعلومات)	**عدد الإشارات الموجبة**	**عدد الإشارات السالبة**	**عدد الأصفار (الحياد)**	**المجموع**	**قيمة z**	**مستوى المعنوية (sig)**	**قيمة الوسيط**
شخص داخل الهيكل التنظيمي في البنك.							
عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي البنك.	47	69	13	129	1.950-	0.0255	4
عدم إلزام الموظفين بأخذ إجازتهم الدورية.	53	54	22	129	0.15	0.5	3
عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد.	44	60	25	129	1.471-	0.0705	3
عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي البنك.	31	73	25	129	4.020-	0	4

مخاطر نظم المعلومات المحاسبية الإلكترونية

عبارات المجال الثاني (أسباب حدوث مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
عدم الوعي الكافي لدى الموظفين بضرورة فحص البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.	38	70	21	129	2.983-	0.0015	4

مستوى المعنوية الإحصائية حسب عند a = 0.05

يلاحظ من خلال الجدول رقم (6) أن قيمة اختبار الإشارة (z) معنوية إحصائياً في كافة العبارات باستثناء العبارات (3, 7, 11, 12)، لم يكن هناك فرقا معنويا احصائيا بين وسيط اراء افراد العينة على هذه العبارات الاربع ووسيط المقياس و هو الدرجة (3)، في حين ان وسيط اراء افراد العينة في باقي العبارات بلغ (4)، و هي تمثل صفة الراي (موافق) حسب المقياس المستخدم في الاستبانة و هو اكبر من وسيط مقياس الاستبانة، و بشكل معنوي احصائيا كما يتضح من قيمة(sig) و هي اقل من (0.05). الامر الذي يني اهمية هذه الاسباب كمسببات للمخاطر التي تهدد نظم المعلزمات المحالسية المحوسبة في المصلارف الفلسطينية.

3 اختبار الفرضية الرئيسة الثالثة والتي نصت على أنه:

لا توجد اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة.

لاختبار الفرضية السابقة؛ فقد تم استخدام اختبار الإشارة لمعرفة ما إذا كانت هناك فروقا معنوية إحصائياً بين وسيط آراء أفراد العينة على المجال الثالث والمتعلق باجراءات الحماية؛ لمواجهة مخاطر نظم المعلومات المحاسبية ووسيط المقياس المستخدم في استبانة الدراسة، وهو الدرجة (3) والذي تمثل صفة (متردد) وذلك لتحديد ما إذا كانت هناك موافقة جوهرية من قبل أفراد العينة على اتباع اجراءات الحماية الواردة في المجال الثالث أم لا.

وأشارت الفرضية الإحصائية العدمية (H0) إلى تردد او عدم موافقة افراد العينة على اجـــراءات الحماية المذكورة، فيما لو كانت آراء أفراد العينة اقل او تساوي الدرجة (3)؛ مما يعنـــي عـــدم توفر اجراءات الحماية في المصارف. أما الفرضية البديلة (H1) فقد أشارت إلى موافقـــة افـــراد العينة على وجود اجراءات الحماية في مصارفهم فيما لو كانت آراء أفـــراد العينـــة اكبـــر مـــن الدرجة(3) . وسيتم اجراء الاختبار الاحصائي و تحديد مستوى المعنوية على اساس ذيل واحد و هو الذيل الاعلى كما هو واضح من الفرضية البديلة السابقة.

جدول رقم (7)

نتيجة اختبار الإشارة للمجال الثالث الخاص باجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة

انواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	الوسيط العام
إجـــراءات الحمايـــة المتبعـــة لمواجهـــة المخاطر التي تهدد نظم المعلومات المحاسبية	2	119	8	129	10.545-	0.000	5

مستوى المعنوية الإحصائية حسب عند a = 0.05

جدول رقم (7) يوضح نتيجة التحليل الخاص بالمخاطرالتي تتعلق بالبيئة. كما يظهر في الجـــدول المذكور، فان قيمة اختبار الإشارة (z) معنوية إحصائياً عند مستوى دلالة (0.05)؛ مما يعني أن هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على اجـــراءات الحمايـــة المتبعـــة؛ لمواجهة مخاطر نظم المعلومات المحاسبية ، ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (3) ويعزز هذه النتيجة أن الوسيط العام لآراء أفراد العينة بلغ (5) وهي تمثـــل درجـــة الموافقة بشدة حسب المقياس المستخدم في استبانة الدراسة. وبالتالي نستنتج من ذلـــك ان افـــراد العينة يرون ان المصارف التي يعملون فيها تتبع اجراءات حماية كافية لمواجهة مخـــاطر نظـــم المعلومات المحاسبية الإلكترونية. وبناء على ذلك نرفض الفرضية البحثية الثالثة و التي نـــصت على انه لا توجد اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونيـــة في المصارف العاملة في قطاع غزة. وللوقوف على اراء افراد العينة حـــول طبيعـــة اجـــراءات الحماية التي تتبعها المصارف العاملة في قطاع غزة بشكل تفصيلي؛ فقد تم إيجاد اختبار الإشـــارة لكل عبارة على حدة من العبارات التي تضمنها المجال الثالث، و المتعلـــق بـــاجراءات الحمايـــة

المتبعة لمواجهة المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية وذلك كما يظهر في الجدول رقم (8).

جدول رقم (8)

نتيجة اختبار الإشارة لكل عبارة من عبارات المجال الثالث الخاص باجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية

عبارات المجال الثالث (اجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
تقوم إدارة البنك بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات.	3	122	4	129	10.554-	0.000	5
تتعهد إدارة البنك العليا لتطبيق أمن المعلومات.	3	117	9	129	10.315-	0.000	5
تتابع إدارة البنك موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة.	5	116	8	129	10.000-	0.000	5
تقوم إدارة البنك بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد.	1	112	16	129	10.348-	0.000	5
تقوم إدارة البنك بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن	3	120	6	129	10.459-	0.000	5

عبارات المجال الثالث (اجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
الرجوع إليها عند الضرورة.							
تطبيق إدارة البنك أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد.	0	123	6	129	11.001-	0.000	5
تقوم إدارة البنك بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة.	5	105	19	129	9.934-	0.000	4
تقوم إدارة البنك بوضع سياسات خاصة بأمن المعلومات تشمل اختيار التقنية المناسبة، والإجراءات اللازمة لجعل هذه التقنية فعالة.	1	116	12	129	10.539-	0.000	5
تقوم إدارة البنك بتركيب طرق الحماية التقنية مثل جدران الحماية (Firewalls) ومضادات الفيروسات وغيرها.	5	113	11	129	9.850-	0.000	5
تقوم إدارة البنك بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا.	5	114	10	129	9.900-	0.000	5

مخاطر نظم المعلومات المحاسبية الإلكترونية

عبارات المجال الثالث (اجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	قيمة الوسيط
تقوم إدارة البنك بفحص طرق الحماية.	3	115	11	129	10.218-	0.000	5
تقوم إدارة البنك باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق.	5	100	24	129	9.173-	0.000	4
تقوم إدارة البنك بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه.	2	109	18	129	10.061-	0.000	5
تستفيد ادارة البنك من خبرة البنوك العالمية في مجال امن المعلومات	7	111	11	129	9,428-	0.000	4

مستوى المعنوية الإحصائية حسب عند a = 0.05

يلاحظ من خلال الجدول رقم (8) أن قيمة اختبار الإشارة (z) معنوية إحصائياً في كافة العبارات؛مما يعني أن هناك فرق معنوي احصائياً بين وسيط آراء أفراد العينة على كل عبارة ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (3)، كما ان وسيط آراء أفراد العينة في جميع العبارات كان (5) باستثناء العبارات (7، 12، 14) فقد كان (4) و هذا يعني ان المصارف العاملة في قطاع غزة تتبع اجراءات الحماية الواردة في الجدول السابق حسب اراء افراد العينة.

9- النتائج و التوصيات

تهدف هذه الدراسة إلى التعرف على المخاطر التى تهدد نظم المعلومات المحاسبية الإلكترونية فى بيئة المصارف العاملة في قطاع غزة ومعدلات تكرارها، و أسباب حدوثها. و كذلك التعرف على اجراءات الحماية التي تتبعها تلك المصارف للحد من المخاطر التي تهدد نظم معلومات المحاسبية الإلكترونية. وقد توصلت هذه الدراسة إلى مجموعة من النتائج والتي من أهمها:

1- اعتماد المصارف العاملة في قطاع غزة في عملها بشكل كبير على النظام الآلي، الا أن هذا

الاعتماد لايتفق مع عدد موظفي تكنولوجيا المعلومات في المصارف حيث تعتمد الفروع على موظف واحد مهمته تشغيل أنظمة الحاسوب بينما الموظفمن المختصون يكون مكانهم في المراكز الرئيسية للفروع وغالبا ما توجد في الضفة الغربية.

2- عدم حدوث مخاطر نظم المعلومات المحاسبية في المصارف العاملة في قطاع غزة، بشكل متكرر، و لكن تعتبر مخاطر الإدخال غير المتعمد واشتراك الموظفين في كلمة السر وتوجيه البيانات والمعلومات إلى أشخاص غير مصرح لهم بذلك؛ اكثر المخاطر تكرارا حيث قد تحدث أكثر من مرة شهريا إلى مرة أسبوعيا.

3- حدوث مخاطر نظم المعلومات المحاسبية الالكترونية ترجع إلى أسباب تتعلق بموظفي البنك نتيجة قلة الخبرة والوعي والتدريب، اضافة إلى أسباب تتعلق بإدارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الاجراءات والأدوات الرقابية المطبقة لدى المصرف.

4- المصارف العاملة في قطاع غزة تتبع اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية.

بعد استعراض نتائج الدراسة فإنه يمكننا الخروج بمجموعة من التوصيات وهي:

1- من الضروري أن تدعم الادارة العليا للمصارف أمن المعلومات لديها وأن تعمل على إنشاء قسم خاص بتكنولوجيا المعلومات في كافة المصارف وتوفير كادر متخصص في تكنولوجيا المعلومات بحيث يكون له مندوبون في الفروع ذوي خبرة وكفاءة عالية لأجل العمل على حماية أمن نظم المعلومات المحاسبية لدى المصارف. و كذلك تطوير قدرات العاملين لديها في مجال امن المعلومات و حمايتها.

2- ضرورة وضع اجراءات تضمن استمرارية عمل وجاهزية نظم المعلومات؛ للعمل في حالة الأزمات من خلال استخدام تجهيزات منيعة أو مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها والحد من وقوعها. وكذلك العمل على تعمية أو تشفير المعلومات عند الحفظ والنقل والتخزين على مختلف الوسائط كي لا يتمكن أحد من اختراقها.

3- وضع ضوابط أمن ورقابة المعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أم اتصالات سلكية ولاسلكية والإنترنت والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية. و وجود خطة حماية أمنية شاملة والتي تنعكس في انخفاض النفقات الناتجة عن توظيف الحلول الجزئية للأمن.

10- المراجع

1- الدهراوي كمال الدين، (2003)، "مدخل معاصر في نظم المعلومات المحاسبية"، الدار الجامعية للنشر والتوزيع، مصر، ط2.

2- عفانة عزو، (1998)، "الإحصاء التربوي: الجزء الثاني، الإحصاء الاستدلالي"، غزة، فلسطين، ط1.

3- Abu-Musa, Ahmad A. (2001), "Evaluating The Security of Computerized Accounting Information Systems: An Empirical Study on Egyptian Banking Industry", PhD. Thesis, Aberdeen University, UK.

4- Abu-Musa, Ahmad A. (2004), "Important Threats to Computerized Accounting Information Systems: An empirical Study on Saudi Organizations" Pubic Administration, A Professional Quarterly Journal Published by The Institute of Public Administration Riyadh, Saudi Arabia, (Vol. 44, No. 3), pp. 1-65.

5- Dhillon, G. (1999), "Managing and controlling computer misuse", Information Management & Computer Security, (Vol. 7, Number 4), PP. 171-175.

6- Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (1992), “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding”, MIS Quarterly, (June), pp. 173 - 186.

7- Ryan, S. D. and B. Bordoloi (1997), “Evaluating Security Threats in Mainframe and Client / Server Environments”, Information & Management, (Vol. 32, Iss. 3), pp. 137 - 142.

8- Siponen, M. T. (2000), “A conceptual Foundation for Organizational Information Security Awareness”, Information Management and Computer Security, Bradford, (Vol. 8, Iss. 8), PP. 31- 44.

9- Whitman Michael E. (2003), "Enemy at the Gate: Threats to Information Security", Communication of the ACM, (Vol. 46, Iss. 8), pp. 91-95.